ARIZONA **D**EPARTMENT **O**F **A**DMINISTRATION	**Statewide** **POLICY**	**State of Arizona**

SOCIAL NETWORKING

DOCUMENT NUMBER:	**P505**
EFFECTIVE DATE:	**DRAFT**
REVISION:	**0.1**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (BU), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statute (A.R.S.)§ 41-3504.

2. PURPOSE

The purpose of this policy is to define proper usage and behavior for Social Networking Applications for BU to further protect the rights and privacy of its citizens and the integrity of the State government.

3. SCOPE

This policy applies to all Budget Units (BUs) and IT integrations and/or data exchange with third parties that perform functions, activities or services for or on behalf of the agency or its divisions. Applicability of this policy to third parties is governed by contractual agreements entered into between BU and the third party/parties.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Exception Procedure.

4.1.1 Existing IT Products and Services

a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services BU subject matter experts shall consider Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.

5.2 BU Assistant Director

a. Conduct a formal assessment of the risk resulting from a Division's use of social networking;

b. Assign appropriate personnel to oversee the use of social networking, evaluate and authorize Agency requests for usage, and determine appropriateness of the content posted to social networking sites; and

c. Periodically review social networking usage to ensure it continues to reflect BU's communication strategy and priorities.

5.3 BU Supervisors shall:

a. Ensure users are appropriately trained and educated on social networking and IT policies;

b. Monitor personnel activities to ensure compliance; and

c. Monitor and filter, as necessary, all social networking content posted and/or viewed.

5.4 Individual BU Enterprise Architecture Users shall:

a. Become familiar with this and related PSPs; and

b. Adhere to all state and BU PSPs pertaining to the use of Social Networking and the State IT resources.

6. STATEWIDE POLICY

This policy establishes and defines the guidelines and use of social media/networking.

6.1 All BU authorized personnel and contractors responsible for content on behalf of BU or the State, who speak officially on behalf of BU or the State, or who may be perceived as speaking on behalf of BU or the State, in social networking efforts, shall:

6.1.1 Receive a copy of A.R.S. § 38-448, as well as acknowledge that any abuse of social media communication and resources may result in discipline or separation from employment.

6.1.2 Receive proper instructions and training, as well as acknowledge their understanding of the Statewide Security P8280, Acceptable User Policy, Division specific policies, and standards and procedures, related to social media/networking, before using any State social media/networking communications.

6.1.3 Obtain approvals from an Assistant Director or BU CIO before registering and participating in social media/networking activity in an official capacity.

6.1.4 Respect copyright laws, intellectual property, and reference/cite sources appropriately.

6.1.5 Understand social media/networking may not be used for personal gain, conducting private commercial transactions, or engaging in private business activities.

6.1.6 Understand that postings to social media/networking websites immediately become part of a public record.

6.1.7 Not post or release proprietary, confidential, sensitive, or other state government Intellectual Property.

6.1.8 Identify themselves appropriately, using agency sanctioned identification, when posting or exchanging information.

6.1.9 Address issues only within the scope of their specific authorization.

6.1.10 Be respectful and mindful of the State, in addition to State leadership, State employees, customers, partners, vendors, citizens, and the public.

6.1.11 Not post information, photos, links or URLs or other items online that would reflect negatively on the State, its citizens or any individual.

6.1.12 BU reserves the right to monitor and log all web social media/networking activity without notice.

6.2 BU Divisions that wish to use social media/networking should develop a brief marketing plan addressing the following:

a. Audience

b. Target Markets

c. Objective

d. Message

e. Measurable metrics that will determine/measure success

f. Management Resources

g. Internal Teams

h. External Management Resources (i.e. contractors)

7. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the BU-ASET website.

8. REFERENCES

8.1 BU Policy P100, Information Technology

8.2 A.R.S. § 41-3504

8.3 Statewide Security P8280, Acceptable User Policy

8.4 Statewide Security Policy P8270 Personnel Security Controls

8.5 Statewide Security Policy P8320 Access Control Policy

8.6 A.R.S. § 38-448

8.7 EO 2008-10, Mitigating Cyber Security Threats

9. ATTACHMENTS

None.